REMARKS

Enclosed herewith is a Substitute Specification incorporating the changes instituted by the Preliminary Amendment filed with the subject application, and in addition, further amending the specification as filed to correct further typographical and grammatical errors.

In support of the above, enclosed herewith is a copy of the specification as filed marked up with the above changes.

The undersigned attorney asserts that no new matter has been incorporated into the Substitute Specification.

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, the claims have been amended for clarity.

The Examiner has rejected claims 1-3, 5-7, 9 and 10 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,553,127 to Kurowski. The Examiner has further rejected claims 4 and 8 under 35 U.S.C. 103(a) as being unpatentable over Kurowski in view of U.S. Patent 6,404,926 to Miyahara et al. In addition, the Examiner has rejected claim 11 under 35 U.S.C. 103(a) as being unpatentable over Kurowski in view of U.S. Patent 6,510,233 to Nakano.

The Kurowski patent discloses a method and apparatus for selective block processing in which blocks in a serial stream of equally sized blocks are selectively watermarked with a watermark

independence on whether the relevant block satisfies or does not satisfy a predetermined criterion.

The subject invention, on the other hand, analyzes a given property of an information signal and determines an actual value of the property, associates different watermarks in a plurality of watermarks with distinct values of the given property, and embeds the watermark from the plurality of watermarks associated with actual value.

Applicants submit that there is only one watermark disclosed or suggested in Kurowski, this one watermark being selectively embedded or not embedded. However, in the subject invention, over the course of time, the embedded watermark changes and, as such, a plurality of watermarks are used, depending on the actual value of the given property of the information signal.

The Miyahara et al. patent discloses an apparatus and method of processing image data, transmission medium, and recording medium, in which, as described at col. 9, lines 46-50, a watermark detector 22 includes a watermark pattern holding memory 32 "In the watermark pattern holding memory 32, the watermark pattern which is the same watermark pattern held in the watermark pattern holding memory 12 (FIG. 26) of the watermark adding device 1 is being held."

In view of the above, it appears that Miyahara et al. only discloses the use of a single watermark. This is supported in Miyahara et al. which states, at col. 9, lines 4-9:

"The watermark adding device 1 in the first embodiment
is configured as shown in FIG> 26, for example, the
same as described above, and as described with
reference to FIGS. 20-23, it will implement a process
such that when the accompanying information signal f is
off, no watermark is added, and when it is on, then the
watermark is added."

The Examiner now states:

"However, Miyahara discloses an apparatus and method of
processing image data in which the embedded watermark
is a combination of two or more basic watermark
patterns (i.e., bits) constituting a set of basic
watermark patterns being selected from different sets
in dependence upon the actual value of the property of
the information signal (i.e., assigning different
watermark patterns based on the threshold value) (Fig.
4, col. 10, lines 5-67 and Col. 11, lines 1-15)."

Applicants submit, however, that the Examiner is mistaken.

This section of Miyahara et al. describes a process for detecting

the watermark in the watermarked signal encoded by the encoder of,

for example, Fig. 1. In particular, this section of Miyahara et al.

is based on Figs. 4 and 5, and describes the operation of the

watermark detector 22 of Fig. 2, and col. 9, lines 10-13 states

"FIG. 2 shows a configuration example of the decoder that decodes

the sign bit train encoded by the encoder shown in FIG. 1." The

cited section of Miyahara et al. discloses the use of a single

watermark which, in steps S2, S4 and S6, is "shifted" by the amounts

0, i and j, respectively. The results of the processing in these

steps is then subjected to median filtering, in which the median

value sum_{med} is found. Applicants submit that it should be clear that

only a single watermark is being detected by the detector 22 of

Miyahara et al., in which the watermark is selectively present

(i.e., turned on or off), and that in order to detect this single

watermark, the detector shifts the watermark by various amounts in

processing the watermarked signal.

Notwithstanding the above, even if one were to group the

"shifted" watermarks as a set of watermarks, then only one set is

being used, and then only to detect the presence of a single

watermark. Applicants submit that this is distinctly different than

that which is claimed in claims 4 and 8, i.e., "each embedded

watermark is a combination of two or more basic watermark patterns

constituting a set of basic watermark patterns, said set of basic

watermark patterns being selected from different sets of basic

watermark patterns in dependence upon the actual value of the

property of the information signal."

Further, Applicants submit that Miyahara et al. does not

supply that which is missing from Kurowski, i.e., over the course of

time, the embedded watermark changes and, as such, a plurality of

watermarks are used, depending on the actual value of the given

property of the information signal.

The Nakano patent discloses an electronic watermark

insertion device which includes a watermark detector for detecting

whether a watermark to be inserted into a signal has already been

inserted into the signal. However, Applicants submit that Nakano

does not supply that which is missing from Kurowski, i.e., over the

course of time, the embedded watermark changes and, as such, a plurality of watermarks are used, depending on the actual value of the given property of the information signal.

In view of the above, Applicants believe that the subject invention, as claimed, is neither anticipated nor rendered obvious by the prior art, either individually or collectively, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-11, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by _Edward W. Goodman_
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as First-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

On _April 13, 2006_

By _Burnett James_

WATERMARK EMBEDDING AND DETECTION

BACKGROUND OF THE INVENTION

Field Of The Invention

[0001]   The invention relates to a method and arrangement for watermarking an information signal, for example, an audio or video
5   signal. The invention also relates to a method and arrangement for detecting a watermark in such an information signal.

~~BACKGROUND OF THE INVENTION~~Description Of The Related Art

[0002]   A known method of watermarking a video signal is
10   disclosed in International Patent Application WO-A-99/45705, corresponding to U.S. Patent Application Serial No. 09/423,273, filed March 2, 1999. In this method, a watermark pattern is added to the video signal. A watermark detector correlates the same pattern with the suspect signal. If the correlation exceeds a given
15   threshold, the pattern is said to be present. The presence or absence of the pattern represents a single bit of information. The embedded watermark may also carry a multi-bit payload. In the system disclosed in WO-A-99/45705, the payload is represented by a combination of one or more basic patterns and spatially shifted
20   versions thereof. The payload is encoded into the respective shift vectors. The watermark detector correlates each basic pattern with the suspect signal, and determines the spatial positions of the

basic patterns with respect to each other. The detector further

checks whether said positions constitute a valid payload.

[0003]   The process of correlating watermark patterns with the

suspect signal requires the watermark detector to have locally

5   stored versions of said patterns. In view thereof, it is desired

that the watermarking system employs only a few different patterns.

The patterns being used are kept secret to the outside world.

However, even without knowledge of the patterns, a hacker can

compromise the system if he has the relevant embedder at his

10   disposal. He/she may feed an arbitrary input signal to said

embedder and subtract the signal from its watermarked version. The

difference signal thus obtained resembles the watermark of any

other watermarked signal, depending on the perception model used in

the watermark embedder at hand. If the difference signal is

15   combined with (e.g., added to or subtracted from) a watermarked

signal, the embedded watermark will substantially be cancelled or

at least no longer represent a valid payload. In either case, the

embedded watermark has been made ineffective.

20   ~~OBJECT AND~~ SUMMARY OF THE INVENTION

[0004]   It is an object of the invention to provide a more secure

method and arrangement for embedding and detecting a watermark in

an information signal, even if a hacker has a watermark embedder at

his/her disposal.

[0005]   To this end, the method in accordance with the invention comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with distinct values of

5   said property, and embedding the watermark associated with said actual value. The corresponding watermark detection method comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with distinct values of

10   said property, and detecting the watermark associated with said actual value.

[0006]   It is achieved with the invention that the embedded watermark pattern changes from time to time, as a function of the information signal content. Feeding an arbitrary signal to an

15   embedder so as to produce a signal that resembles the watermark, as described above, does not work anymore because the arbitrary signal has different properties. A significant advantage of the invention is that the number of different watermark patterns which the detector must store can be kept much lower. Said number is a result

20   of balancing detector complexity versus security.

[0007]   There are numerous examples of properties of the information signal that can be used for selecting the watermark pattern to be embedded. The only requirement to be fulfilled is its robustness or invariance with respect to the embedded watermark.

25   Advantageous examples of properties are distinct distributions of

luminance values of a video signal, or distinct shapes of the
frequency spectrum of an audio signal.

[0008] Further aspects of the invention are apparent from and
will be elucidated with reference to the embodiments described
5 hereinafter. The examples relate to watermark embedding and
detection of video signals, but it will be appreciated that the
invention equally applies to audio signals or any other type of
multimedia signal.

10   BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Fig. 1 shows, schematically, a block diagram of a
watermark embedder in accordance with the invention.;

[0010] Fig. 2 shows, schematically, a block diagram of a
watermark detector in accordance with the invention.;

15 [0011] Fig. 3 shows an arrangement to illustrate illustrating
the operation of the watermark embedder and detector.;

[0012] Figs. 4 and 5 show block diagrams of further embodiments
of the watermark embedder in accordance with the invention.; and

[0013] Fig. 6 shows a block diagram of a further embodiment of
20 the watermark detector in accordance with the invention.

               DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Fig. 1 shows, schematically, a block diagram of an
embodiment of a watermark embedder 1 in accordance with the
25 invention. It will here be assumed that the embedded watermark

represents a 1-bit payload. For example, the absence of a watermark indicates that the video signal may freely be copied, whereas the presence of a predetermined watermark denotes that making a copy of the signal is prohibited.

5   [0015]   The embedder_1 receives an input video signal I in the form of a sequence of images, and comprises an adder 11 which adds a watermark pattern W_i to each image. The embedder_1 further comprises an image analyzer 12, a selector 13 and a read-only memory 14 in which a plurality of different watermark patterns

10    $W_1...W_N$ are stored. The analyzer 12 receives the video signal and analyzes a given property P of the video signal as a function of time. The actual value of property P found by analyzer 12 is applied to the selector 13. In response thereto, the selector_13 selects_and applies one of the stored watermark patterns $W_1...W_N$ to

15   the adder 11 for embedding.

[0016]   The analyzer 12 may take numerous forms. A few examples will be given to provide sufficient teaching to enable a skilled person to design appropriate alternative embodiments. The property being analyzed may be the distribution of luminance values across

20   the image (spatial distribution) or across a sequence of images (temporal distribution). In a first example, the analyzer divides each image into sub-images, and determines which of said sub-images has the highest average luminance. The relevant sub-image number is the actual value of property P. In a second example, the analyzer

25   assigns a "0" to each sub-image having a low average luminance and

a "1" to each sub-image having a high average luminance. Each video

image is now characterized by an n-bit code, where n is the number

of sub-images. The relevant n-bit code is the actual value of

property P. The property being analyzed may also be local image

5   activity. Such an analysis can easily be carried out in the

frequency domain.

[0017]   Fig. 2 shows, schematically, a block diagram of a

preferred embodiment of a watermark detector 2 in accordance with

the invention. The detector 2 receives a suspect video signal J and

10   comprises an image analyzer 22, a selector 23 and a read-only

memory 24 which are identical to the corresponding counterparts of

embedder 1. Accordingly, the analyzer 22 analyzes the same property

P of the video signal, and the selector 23 selects the same

watermark pattern W from the stored patterns $W_1...W_N$, as selected in

15   the embedder 1.

[0018]   The detector 2 further comprises a correlation circuit 21

which calculates the correlation between each image of the suspect

video signal and the applied watermark pattern W_i. If the

correlation exceeds a predetermined threshold, the selected

20   watermark pattern W_i is said to be present (D=1), otherwise, it is

said to be absent (D=0).

[0019]   The correlation circuit 21 is preferably of a type which

performs the correlation for all possible spatial positions of the

applied watermark with respect to the image. Such a correlation

25   circuit is disclosed in International Patent Application WO-A-

99/45705. ~~It~~ The correlation circuit generates a correlation

pattern which exhibits a peak for each spatial position of the

watermark. WO-A-99/45705 describes that multiple peak positions may

represent a payload. However, as mentioned above, the payload in

5   this example is a 1-bit copy control signal. The detection circuit

2 will consider the presence of 2 or more peaks as an invalid

payload (D=0).

[0020]   It is assumed that the watermark patterns $W_1...W_N$ are

secret and can neither be retrieved by interrogating the embedder

10   or detector circuits. As will now be explained with reference to

Fig. 3, the invention prevents a hacker from compromising the

system when he/she happens to have an embedder at his/her disposal.

In Fig. 3, a potential hacker receives a video signal V' ~~being~~

having been watermarked by an embedder 1a. The signal V' may be a

15   recorded signal, in which case, the actual embedding took place a

long time ago. The embedder 1a is of a type as described above with

reference to Fig. 1.

[0021]   The hacker has an identical embedder 1b at his/her

disposal. An arbitrary video signal X is applied to said embedder

20   1b so as to locally generate a watermarked video signal X'. An

adder 3 subtracts the arbitrary signal X from its watermarked

version X'. The difference signal (which strongly resembles the

embedded watermark pattern) is then combined with (added to or

subtracted from) the watermarked signal V' by a further adder 4.

The suspect signal V'' thus processed is applied to a watermark

detector 2 as described above with reference to Fig. 2.

[0022]   Without the provisions of the invention, both embedders

1a and 1b embed the same watermark in the respective input signals.

5   This results either in a cancellation of the watermark in the

suspect signal V'' or in an invalid payload due to multiple

occurrences of the watermark pattern W at different positions. In

both cases, the detector generates an output signal D=0 and the

hacking attack is successful.

10   [0023]   With the provisions of the invention, the watermark W_i

(i=1..N) in signal V' will generally differ from the watermark W_j

(j=1..N) in signal X', because the contents of the original video

signals V and X are different. The property analysis algorithm of

detector 2 responds to the contents of signal V'' which is

15   substantially equal to the contents of V. Consequently, the

watermark pattern being checked by detector 2 is the watermark

pattern W_i which has been embedded by embedder 1a. The detector

ignores the additional presence of a different pattern W_j, and the

hacking attack thus fails.

20   [0024]   A possible work-around is feeding the watermarked signal

V' instead of an arbitrary signal X to embedder 1b, so as to force

embedder 1b to select the same watermark W_i as embedder 1a. To

avoid this, the embedders 1a and 1b are preferably of a type that

refrains from embedding a watermark in a signal that has already

25   been watermarked. Fig. 4 shows a schematic block diagram of such an

embedder. ~~It~~ The embedder comprises the same adder 11, image

analyzer 12, selector 13 and ROM 14 as the embedder 1 ~~which is~~

shown in Fig. 1. ~~It~~ The embedder further comprises the correlation

circuit 21 of the detector ~~which is~~ 2 shown in Fig. 2. The

5 correlation circuit 21 detects whether the input signal I already

includes the watermark pattern W_i to be embedded. If that is the

case (D=1), a switch 15 is controlled to prevent the watermark

pattern W_i from being embedded multiple times.

[0025]   Fig. 5 shows a schematic block diagram of a watermark

10 embedder for embedding a multi-bit payload in the video signal. The

embedder comprises the same adder 11, image analyzer 12, selector

13 and ROM 14 as described before with reference to Fig. 1. The ROM

14 now stores a plurality of sets of watermark patterns. The

embedder further includes an encoding circuit 16 which receives a

15 selected set i of basic watermark patterns $W_{i,1}$, $W_{i,2}$, ..., and

encodes a multi-bit payload d into the relative positions of said

patterns. The basic patterns have a relatively small size (e.g.,

128x128 pixels). The watermark pattern generated by encoder 16 is

subsequently tiled over the image by a tiling circuit 17. The ROM

20 14 stores different sets of basic patterns for different values of

signal property P. The actual set of basic patterns being applied

to encoder 16 is controlled by the actual value of property P and

changes as a function of time.

[0026]   Fig. 6 shows the corresponding watermark detector. The

25 detector comprises a folding circuit 25 for folding and storing

image segments of 128x128 pixels in a buffer prior to correlation.
The detector further comprises the same correlation circuit 21,
image analyzer 22, selector 23 and read only memory 24 as described
before with reference to Fig. 2. The ROM 24 stores different sets

5   of basic patterns for different values of signal property P. The
actual set of basic patterns being applied to the correlation
circuit 21 is controlled by the actual value of property P.

[0027]   It should be noted that the invention is not limited to
the watermarking systems described in the embodiments. For example,

10   a watermarking system is known that uses n different watermark
patterns, each pattern corresponding to one bit of an n-bit
payload. In accordance with this invention, the embedder and
detector of such a system include different sets of n patterns. A
particular set is then selected in response to the actual value of

15   a signal property.

[0028]   In summary, a method and arrangement for embedding and
detecting a watermark in an information signal is disclosed. The
embedded watermark (W_i) is selected (13) from a plurality of
watermarks ($W_1..W_N$) in dependence upon a property P of the signal.

20   An example of such a property is the distribution of luminance
values of the current video image as calculated by an analysis
circuit (12). The corresponding watermark detector performs the
same operation: the watermark being looked for depends on the same
signal property. It is achieved with the invention that the

embedded watermark changes from time to time as a function of the
information signal content, so that it cannot easily be hacked.

ABSTRACT÷OF THE DISCLOSURE

A—In a method and arrangement for embedding and detecting
a watermark in an information signal—is disclosed. The, the
5   embedded watermark (W_i) is selected (13) from a plurality of
watermarks ($W_1..W_N$) in dependence upon a property P of the signal.
An example of such a property is the distribution of luminance
values of the current video image as calculated by an analysis
circuit (12). The corresponding watermark detector performs the
10   same operation: the watermark being looked for depends on the same
signal property. It is achieved with the invention that the
embedded watermark changes from time to time as a function of the
information signal content, so that it cannot easily be hacked.

15   Fig. 1